

NXP Semiconductors ATBK

Site Security Target

Rev. 2.5 — 29 September 2025

NXPOMS-1719007347-2664

Evaluation document

PUBLIC

Document information

Information	Content
Keywords	Common Criteria, Manufacturing, NXP ATBK, Site Security Target
Abstract	Site Security Target for the site certification of the site Assembly and Test Bangkok (ATBK)



1 Document Information

1.1 Reference

Title: Site Security Target - NXP Assembly & Test Bangkok ATBK
Version: 2.5
Date: 29 September 2025
Company: NXP Semiconductors Thailand Ltd.
Name of the site: NXP Semiconductors ATBK
Site Type: Test
Assembly
Failure Analysis
Reliability Testing
Internal Shipment
Warehouse with External Delivery
Satellite
EAL: EAL6

1.2 Revision History

Rev.	Date	Description	Author	Owner
2.3	2025-01-29	New release due to change of ITSEF (IT Security Evaluation Facility) and CB (Certification Body). All prior revisions were archived.	Panagiotis Afratis	Michael Sandu
2.4	2025-09-10	Updates due to certification audit, resolving inconsistencies in section 2.2.	Panagiotis Afratis	Michael Sandu
2.5	2025-09-29	Updates due to certification, withdrawal of ALC_TAT.	Panagiotis Afratis	Michael Sandu

2 SST Introduction

This document is based on the Eurosmart Site Security Target Template [1] with adaptations such that it fits the site.

This Site Security Target is intended to be used by only one specific client, namely NXP Semiconductors B.V.. Therefore, the term 'client' in this document refers directly to NXP Semiconductors B.V..

Definitions of the color coded areas and handling instructions for classified material can be found here [2]

In the following chapters you will find several times statements like 'this and/or that'. The applicability is given by the 'type of site' and the definition of assets.

2.1 Identification of the Site

The site NXP Semiconductors ATBK is located at:

NXP Semiconductors Thailand Ltd. (ATBK)

303 Moo 3 Chaengwattana Rd. Laksi,

Bangkok 10210

Thailand

2.2 Site Description

2.2.1 Physical Scope

All areas in scope are classified as YELLOW and RED areas. These areas will be within the following buildings.

- Building A (1st floor, 2nd floor)
- Building C (1st floor, 2nd floor)
- Building E (1st floor, 2nd floor, Mezzanine 2nd, 4th floor)
- Industrial Warehouse (1st, Mezzanine, 2nd, 3rd)
- Security Operations Center (SOC)

A more detailed view of the layout is described in documentation referenced into the Site Security Manual (SSM) for ATBK.

Those locations contain security areas with restricted access where only authorized persons are allowed to enter.

Within those areas, only authorized people are entitled to access sensitive information.

To enforce such access restriction, a combination of physical, procedural, personnel and logical measurements have been installed.

2.2.2 Logical Scope

The following life-cycle phases as defined in 'Security IC Platform Protection Profile with Augmentation Packages' (PP-0084) are subject of the SST:

- Phase III: IC Manufacturing
- Phase IV: IC Packaging

To perform its development activities the site uses the NXP CCC&S provided and managed remote IT-infrastructure. Locally available IT equipment like workstations or VPN router is also provided and managed

by NXP CCC&S directly. The site works as per NXP CCC&S processes. CCC&S is the abbreviation for 'Competence Center Crypto & Security'. The site works according to NXP ICC&S processes.

IT Manufacturing provides a Secure Production Network IT infrastructure and Trust

Provisioning provides test control, Fabkey, ROMCode and Serial number in order to facilitate the secure test process. The Secure Manufacturing Network is established in line with the same compliance requirements as CCC&S product development process.

The following services and/or processes provided by NXP ATBK are in the scope of the site evaluation process. Some processes are directly part of the phases presented before and others are supporting processes which can be involved at any phase of the production.

Supporting service

- Security (SOC)
- IT support including TP OPS (SCA) (Building C-2)
- Warehousing (Building IWH)
- Scrapping (Building A-1, E-1, E-2)
- Delivery and shipment (Building IWH).

2.2.3 List of services in Scope

The following services and/or processes provided by the site are in the scope of the site evaluation process. Some processes are directly part of the phases presented before and others are supporting processes which can be involved at any phase of the development. The services are detailed in section [Section 8.2](#).

- IC Manufacturing (Phase 3) under MES2 Camstar system;
- Die/Wafer rooms (Building E-1, E-2, E-4)
 - Die room
 - Wafer storage #5
 - Wafer storage #6
- Product Engineer/ Test Engineering (Building A-1)
 - Development and support of test program development, sustaining, and support activities for BLs.
- Wafer Test (Building E-4)
 - Input program into wafer according customer requirement if relevant (download of Secure IC embedded software).
 - Input data according to Trust Provisioning service used.
 - Functional wafer test of security products (test program execution)
 - Development of tools to facilitate tests centers activities using system box systems (SB-9).
 - Support users from internal and external test centers users (1st and 2nd line support).
 - Thin Wafer Testing - TWTT
- Product Diagnostic & Quality Center - Failure Analysis and Reliability (Building C-1)
 - Perform first failure analysis to find root causes of defects related to security or not.
 - Problem Solving Services for Sustaining activities and package innovation for any NXP department worldwide. (Reliability qualification and monitoring)
This service comprises the handling of customer return.
- Final Test (Buildings A-2, E-1)
 - Download of secure IC embedded software (if relevant)

- Final testing before send to packing process by magnetizing or electrical test.
- IC Packaging (Phase 4) under MES Camstar system;
 - Pre-Assembly (Building E-2)
 - Preparing die and wafer before sending to assembly process by grinding, mounting and sawing
- Assembly activities (Integrated Circuit Module 3 (ICM) (Building E-1), TWTT (Building E-4), QFN (Building E-4), Bare Die (Building E-2), Packing (Building A-1))
 - Assembly plastic leadless module carrier, contactless & contact dual interface chip card and leaded stick.
 - Covering or stuffing for shipping. Before release lots to IWH.
- Network rooms (Buildings A-1, EM1-2, EM2, EM4-1, EM4-2)

3 Conformance Claim

The SST is conformant to Common Criteria Version 2022 ([\[4\]](#), [\[5\]](#), [\[6\]](#), [\[7\]](#)).

For the evaluation the following methodology will be used:

- Common Methodology for Information Security Evaluation (CEM), Evaluation Methodology; Version 2022 ([\[8\]](#))
- Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1); Version 2024 ([\[9\]](#))

The evaluation of the site comprises the following assurance components:

- **ALC_CMC.5**
- **ALC_CMS.5**
- **ALC_DVS.2**
- **ALC_LCD.1**
- **ALC_DEL.1**

The assurance level chosen for the SST is compliant to the Security IC Platform Protection Profile [\[3\]](#) and is therefore suitable for the evaluation of (software for) Security ICs.

The chosen assurance components are derived from the assurance level EAL6 of the assurance class "Life-Cycle Support". For the assessment of the security measures attackers with a high attack potential are assumed. Therefore, this site supports product evaluations up to EAL6.

4 Security Problem Definition

The Security Problem Definition comprises security problems derived from threats against the assets handled by the site and security problems derived from the configuration management requirements. The configuration management covers the integrity of the TOE and the security management of the site.

4.1 Assets

Depending on the setup of the Site, the protection of the following assets is needed:

Physical Security Objects: The site has physical security objects in relation to the "intended TOEs". Both the integrity and the confidentiality of these must be protected.

- Printed Security Documents
- Wafers and Dies
- Scrap Material (for final destruction)
- IC Packages
- Security Seal Tape
- IT Infrastructure (e.g. VPN, Switches, Network Components, Servers)

Development Data: The site has access to or even copies of electronic development data in relation to developed TOEs. Both the integrity and the confidentiality of these electronic documents must be protected.

- Chip Design Data (e.g. Layout)
- Chip Development Documents (e.g. Design Report)
- Failure Analysis Reports

Cryptographic Keys: The site creates, receives and/or handles cryptographic keys. Both the integrity and the confidentiality of these electronic data must be protected. The Cryptographic Key material can be present on:

- Network Devices (e.g. router keys to establish a secure connection)
- Pre-Personalisation Data

Product Configuration Data: The site has access to product configuration data in relation to intended TOEs.

- Product Specification Data (e.g. Wafer and Assembly/Package Specification)
- Pre-Personalisation Data (e.g. FabKey Data, OEF Customer Data)
- Test Program

Site Certification Data: The site has access to documentation needed to successfully pass a site certification. Both the integrity and the confidentiality of this data must be protected.

- Site Security Manual
- Configuration List (Documents)

4.2 Threats

T.Smart-Theft: An attacker tries to access sensitive areas of the site for manipulation or theft of sensitive assets. The attacker has sufficient time to investigate the site outside the controlled boundary. For the attack the use of standard equipment for burglary is considered. In addition, the attacker may be able to use specific working clothes of the site to camouflage the intention.

T.Rugged-Theft: An experienced thief with specialised equipment for burglary, who may be paid to perform the attack tries to access sensitive areas and manipulate or steal sensitive assets.

T.Computer-Net: A hacker with substantial expertise, standard equipment, who may be paid to attempt to remotely access sensitive network segments to get access to development and/or production systems

with the intention to modify the development and/or production process thus violating integrity and possibly confidentiality.

T.Accident-Change: An employee, contractor or student trainee may exchange products of different production lots / different clients during production or changes tool configuration that have an impact on the "intended TOE" by accident.

T.Unauthorised-Staff: Unauthorised employees or subcontractors get access to assets or systems used for development, configuration management and/or production, so that the confidentiality and/or the integrity of the "intended TOE" is violated. This can apply to any development and/or production step and any asset related to the "intended TOE" or its configuration.

T.Staff-Collusion: An attacker tries to get access to assets handled at the site. The attacker tries to get support from one employee through an attempted extortion or an attempt at bribery.

T.Attack-Transport: An attacker might try to get hold of any assets during the internal shipment and/or the external delivery. The target is to compromise confidential information or violate the integrity of the assets during the shipment/delivery process to allow a modification, cloning or the direct/indirect retrieval of confidential information.

4.3 Organisational Security Policies

P.Config-IT_Env: In addition to the used software on development and/or production workstations and servers, the site uses configuration management systems for file versioning and problem tracking. For file versioning and problem tracking, the team members are assigned to project specific, centralized repositories to support proper management of multiple products and the site internal procedures. The team members are requested to use only project related IT equipment with the provided tools.

P.LifeCycle-Doc: The site uses life cycle documentation that describe:

1. Description of configuration management systems and their usage;
2. A configuration items list;
3. Site security;
4. The production/development process;
5. The production/development tools.

P.Config-Items: The configuration management system shall be able to uniquely identify all configuration items. This includes the unique identification of items that are created, generated, developed or used at a site as well as the received and transferred and/or provided items.

P.Config-Control: The procedures for setting up the production and/or development process for a new product as well as the procedure that allows changes of the initial setup for a product is only applied by authorised personnel. Automated systems support the configuration management and ensure access control or interactive acceptance measures for set up and changes. The procedure for the initial set up of a production and/or development process ensures that sufficient information is provided by the client.

P.Config-Process: The services and/or processes provided by the site are controlled in the configuration management plan. This comprises incoming items, tools used for the development and/or production of the product, the management of flaws and optimizations of the process flow as well as the documentation that describes the services and/or processes provided by the site. A released production/development process is defined and under version control.

P.Reception-Control: The inspection of incoming items done at the site ensures that the received assets comply with the properties stated by the client. Furthermore, it is verified that the "intended TOE" can be identified and a released process is defined for the "intended TOE". If applicable this aspect includes the check that all required information and data is available to handle the incoming items.

P.Accept-Product: The testing and quality control of the site ensures that the released "intended TOE" comply with the specification agreed with the client. The acceptance process is supported by automated measures. Records are generated for the acceptance process of the assets. Thereby, it is ensured that the properties of the "intended TOE" are ensured when internally shipped/externally delivered.

P.Zero-Balance: The site ensures that all sensitive items (security relevant parts of the "intended TOEs" of different clients) are separated and traced on a device basis. For each handover, either an automated or an organizational "two-employees-acknowledgement" (four-eyes principle) is applied for functional and defect assets. As per the released production process the defect assets are either destroyed at the site or sent back to the client.

P.Organise-Product: The development, configuration, pre-personalisation, initialisation or personalisation process is applied as specified by the client. If the data includes sensitive items like keys relevant for the life-cycle or configuration data that affect the security of the "intended TOE", appropriate measures are in place. This includes the requirement that the knowledge of sensitive keys is split to at least two different persons. Furthermore, technical measures like crypto-boxes, separation of network, split access permission and secure storage is implemented for this kind of data.

P.Product-Transport: Technical and organisational measures ensure the correct labelling of the "intended TOE". A controlled internal shipment and/or the external delivery is applied. The transport supports traceability up to the recipient. If applicable or required, this policy includes measures for packing to protect the product during transport.

P.Data-Transfer: Any data in electronic form (e.g. keys, initialization data, design data, job deck, product specifications, test programs, test program specifications, release information etc.) that is classified as sensitive or higher security level by the client is encrypted to ensure confidentiality of the data. In addition, measures are used to control the integrity of the data after the transfer.

P.Scrap-Items: Any item that is defect, end-of-life or that does not comply with the quality requirements is shipped back to the client for destruction or is scrapped at the site in a way that the destructed item does not support any attacker.

4.4 Assumptions

Each site operating in a production flow must rely on preconditions provided by the previous site. Each site must rely on the information received by the previous site/client. This is reflected by the assumptions that must be defined for the interface.

A.Secure-IT-Provisioning: The local IT equipment (e.g. workstations, servers, HSMs) is connected to a secure remote IT-Infrastructure through a secure (encrypted) network connection. The local secure IT-infrastructure together with the remote secure IT-infrastructure and the secure connection between them will satisfy all relevant ALC requirements and are provided and managed by the client. The workstations are configured such that any logical assets are contained within encrypted containers.

NXP rationale for usage of this site: *The secure connection is established by using a VPN tunnel between the two sites. The underlying connection is a rented line which additionally provides an encryption on its own. The evaluator was informed during connection of this site to the security certified network infrastructure. The correctness of the implementation was checked during the virtual Master IT audit. Please refer to the site visit report [11]. The standard NXP Semiconductors PC/Laptop stream developed during the 'Tightening security project' supports the usage of encrypted containers. The usage of this tool is introduced to every user during the Advanced Security Awareness Training.*

A.Client-Agreements [Production]: The site participates in the production of products. For each product the site and the client agree on the following items:

- the activities to be performed by the site,
- the specifications of the input for the site including tools,

- the acceptance of the results by the client,
- the handling of scrap configuration items: in case that scrap is not destroyed by the site, scrap configuration items are transferred back to the client.

The agreed methods and tools ensure the correct handling of the configuration items in terms of Common Criteria regarding the classes ALC_CMC, ALC_CMS.

NXP rationale for usage of this site: Each product is clearly defined in the corresponding product specification, wafer specifications, production process specification, test specifications (especially the electrical test specification), bond plans, package specification, wafer maps and many more. Test programs ensure various checks, up to the functional verification of the IC. This site receives those inputs as required to adapt/control their production process. Final ICs are quality checked at NXP and undergo characterization and reliability tests. In case discrepancies are found, this site will get feedback to adjust and improve their production process.

A.Client-Agreements [Test]: The site participates in the failure analysis and/or reliability testing of products. For each product the site and the client agree on the following items:

- the activities to be performed by the site,
- the specifications of the input for the site including tools (e.g. definitions, scripts, process limits, process parameters, test requirements, test limits), which are secured by reasonable means against modification and/or disclosure, if necessary,
- the classification of the documents.

The agreed methods and tools ensure the correct handling of the configuration items in terms of Common Criteria regarding the classes ALC_CMC, ALC_CMS.

NXP rationale for usage of this site: All data in electronic form will be transferred to and stored at the site according to NXPOMS-1719007347-2401 "CCC&S Security Objects". Necessary information and documents to be exchanged, can be found here NXPOMS-999116894-3989 "L-BL CS BCaM Handbook".

A.Client-Agreements [Warehouse]: The site participates in the forwarding of products. The site and the client agree on the following items:

- the activities to be performed by the site including work instructions (e.g. handling instructions, packing instructions)
- the pre-alert message (including delivery note, air waybill, security seal information) for each shipment via the agreed tools,
- the item identification and classification,
- the delivery and shipment details of any security relevant item,
- the handling of scrap configuration items: in case that scrap is not destroyed by the site, scrap configuration items are transferred back to the client,
- in case of necessary updates to the life cycle documentation, the site and the client align.

The agreed methods and tools ensure the correct handling of the configuration items in terms of Common Criteria regarding the classes ALC_CMC, ALC_CMS and ALC_DEL.

NXP rationale for usage of this site: The delivery and shipment is covered by NXPOMS-1719007347-2354 "CCC&S Packing and Delivery Requirements for Security Products" with all relevant information and handling instructions, while the return shipment (also scrap) from this site to NXP is covered in their ALC-DVS documentation.

A.Client-Agreements [Satellite]: The site participates in the development of products. The site and the client agree on the following items:

- the activities to be performed by the site,
- the specifications of the input for the site including tools,
- the acceptance of the results by the client,

- the used configuration management methods, tools and their setup,
- the delivery and shipment details of any security relevant item,
- the necessary setup of computers, their configuration and user accounts,
- the handling of scrap configuration items: in case that scrap is not destroyed by the site, scrap configuration items are transferred back to the client,
- in case of necessary updates to the life cycle documentation, the site and the client align.

The agreed methods and tools ensure the correct handling of the configuration items in terms of Common Criteria regarding the classes `ALC_CMC`, `ALC_CMS`.

NXP rationale for usage of this site: *Whether the team members are located on an NXP premise or remotely on another secure site does not make any difference. They are part of the team and contribute in the same way as all team members do. All available security objects are handled according to NXPOMS-1719007347-2401 "CCC&S Security Objects". All activities per site are covered in the overall PMP, the sub-project PMP or the WBS in Sciforma as documented in NXPOMS-999116894-3989 "L-BL CS BCaM Handbook". The input for the site is handled during the project setup and the creation of the WBS for the engineers at the site. The acceptance of the results is defined during the project setup in the requirements development phase and checked during the gate reviews. The used configuration management methods and tools are documented in NXPOMS-1719007347-2524 "Configuration and Data Management Procedure". The delivery and shipment is covered by NXPOMS-1719007347-2354 "CCC&S Packing and Delivery Requirements for Security Products", while the return shipment (also scrap) from this site to NXP is covered in their ALC-DVS documentation. This site is supported by the NXP IT team to put in place and to configure development and production computers according to corporate and/or CCC&S rules. They use the usual configuration management tools which were certified during the virtual Master IT audit.*

A.Client-Agreements [FA]: The site participates in the failure analysis and/or reliability testing of products. For each product the site and the client agree on the following items:

- the activities to be performed by the site,
- the specifications of the input for the site including tools (e.g. definitions, scripts, process limits, process parameters, test requirements, test limits), which are secured by reasonable means against modification and/or disclosure, if necessary,
- the classification of the documents.

The agreed methods and tools ensure the correct handling of the configuration items in terms of Common Criteria regarding the classes `ALC_CMC` and `ALC_CMS`.

NXP rationale for usage of this site: *All data in electronic form will be transferred to and stored at the site according to NXPOMS-1719007347-2401 "CCC&S Security Objects". Necessary information and documents to be exchanged, can be found here NXPOMS-999116894-3989 "L-BL CS BCaM Handbook".*

A.Data-Transfer [Test]: The client must provide test data and optional pre-personalisation data via a secure connection to the site in correct data format. The client is responsible for the secure transfer of data into the site's secure network. The data must be prepared in a way, so that the site is able to directly get the data from the client in order to process it using their testers.

NXP rationale for usage of this site: *Alignment on tester type and specification is done for products which are foreseen to use wafer test service. NXP provides a GPG encrypted test program with all required information via SFTP. Decryption and installation at the site is done according to the certified procedure.*

A.Item-Identification: Each configuration item received by the site is appropriately labelled to ensure the identification of the configuration item.

NXP rationale for usage of this site: *The site uses commonly used tools in NXP. They all were found suitable for proper configuration item handling and providing unique identifiers.*

A.External-Delivery: The recipient (consumer) of the product is identified by the address provided by the client. The address of the consumer is part of the product setup.

NXP rationale for usage of this site: All shipments follow the same procedures. A shipment request is generated per paper, database, website or per mail. After approval (e.g. by security management, export control, group leader, cost center manager,...) such request is entered/transferred in to SAP where a shipment address must exist for the recipient. Every new external development or production site has to be added once to the SAP system, before it can be used. The address is determined during project setup or site certification request. The secure shipment process from that moment on is according to the process documentation in NXPOMS-1719007347-2354 "CCC&S Packing and Delivery Requirements for Security Products".

A.Mask-Support [Assembly]: The client must provide appropriate masks for the assembly that are compliant with the assembly process released at the site. Further the masks must include identification data that fits to the production support of the site. In addition, the client must support the maintenance of the masks and the scrap of obsolete masks.

NXP rationale for usage of this site: NXP provides GDS data for the RDL and placement of balls. The site runs DRC, checks for optimizations and provides data back to NXP for approval. After approval by NXP they order the mask. All data transfer is done GPG encrypted.

A.Internal-Shipment: The recipient (client) of the product is identified by the address of the client site. The address of the client is part of the product setup.

NXP rationale for usage of this site: All shipments follow the same procedures. A shipment request is generated per paper, database, website or per mail. After approval (e.g. by security management, export control, group leader, cost center manager,...) such request is entered/transferred in to SAP where a shipment address must exist for the recipient. Every new external development or production site has to be added once to the SAP system, before it can be used. The address is determined during project setup or site certification request. The secure shipment process from that moment on is according to the process documentation in NXPOMS-1719007347-2354 "CCC&S Packing and Delivery Requirements for Security Products".

A.Product-Integrity: The self-protecting features of the devices are fully operational, and it is not possible to influence the configuration and behaviour of the devices based on insufficient operational conditions or any command sequence generated by an attacker or by accident.

NXP rationale for usage of this site: Two different approaches ensure that all devices are integrity protected:

* On arrival of the secure product at the site, all wafer testing is already complete. The devices on the wafer are in application mode. This means self-protecting features are activated and access to secure data is blocked for the site and NXP - at that stage the product is a "black box" only.

* The self-protecting features of the device are verified by the test program. If the test program detects an unexpected configuration or behaviour the device is marked as fail device and scrapped under zero balancing control.

5 Security Objectives

The Security Objectives are related to physical, technical, and organizational security measures, the configuration management as well as the internal shipment and/or the external delivery.

O.Config-IT_Env: In addition to the used software on development workstations/systems and servers, the site uses configuration management systems for file versioning and problem tracking. For file versioning unique repositories are used to support proper management of multiple products and the site internal procedures.

O.Exclusive-Access: The only way to access the clients network is through management workstations connected to the encryption equipment provided by the client. There is no internal network access to the encryption equipment.

O.LifeCycle-Doc: The site uses life cycle documentation that describes:

1. Description of configuration management systems and their usage;
2. A configuration items list;
3. Site security;
4. The manufacturing process;
5. The manufacturing tools;
6. Configuration Management Plan.

O.Physical-Access: The combination of physical partitioning between the different access control levels together with technical and organisational security measures allows a sufficient separation of employees to enforce the "need to know" principle. The access control shall support the limitation for the access to these areas including the identification and rejection of unauthorised people. The site enforces two or three levels of access control to sensitive areas of the site. The access control measures ensure that only registered and authorized people can access restricted areas. Sensitive products and data are handled in restricted areas only. Network cabling is protected according to classification of the transferred data by avoiding routes through public areas or by usage of appropriate cryptographic measures.

O.Security-Control: Assigned personnel of the site or guards operate the systems for access control and surveillance and respond to alarms. Technical security measures like video control, motion sensors and similar kind of sensors support the enforcement of the access control. These personnel are also responsible for registering and ensuring escort of visitors, contractors and suppliers.

O.Alarm-Response: The technical and organisational security measures ensure that an alarm is generated before an unauthorised person gets access to any sensitive configuration item (assets). After the alarm is triggered the unauthorised person still has to overcome further security measures. The reaction time of the employees and/or guards is short enough to prevent a successful attack.

O.Internal-Monitor: The site performs security management meetings at least every six months. The security management meetings are used to review security incidences, to verify that maintenance measures are applied and to reconsider the assessment of risks and security measures. Furthermore, an internal audit is performed every year to control the application of the security measures. Sensitive processes may be controlled within a shorter time frame to ensure a sufficient protection.

O.Maintain-Security: Technical security measures are maintained regularly to ensure correct operation. The logging of sensitive systems is checked regularly. This comprises the access control system to ensure that only authorised employees have access to sensitive areas as well as computer/network systems to ensure that they are configured as required to ensure the protection of the networks and computer systems.

O.Network-Separation: The development network of the site exists within the secured areas of the site only. It is connected only to:

1. the VPN gateway that provides a secure connection to the remote secure network of the client;
2. the development workstations provided by the client;

3. additional equipment (e.g. a printer) approved by the client.

O.Logical-Access: The site implements a firewall system to enforce a logical separation between the internal network and the internet. The firewall system ensures that only defined services and defined connections are accepted. Furthermore, the internal network is separated into production networks, office and administration network. Specific networks for production and configuration/administration are further logically separated from other internal network to enforce access control. Access to the production network and related systems is restricted to authorised employees involved in the configuration tasks of the production systems. Every user of an IT system has its own user account and password. An authentication using a unique user account and password is enforced by all computer systems.

O.Logical-Operation: All network segments and the computer systems are kept up to date (software updates, security patches, virus protection, spyware protection). The backup of sensitive data and security relevant logs is applied according to the classification of the stored data.

O.Config-Items: The site has a configuration management system that assigns a unique internal identification to each product to uniquely identify configuration items and allow an assignment to the client. Also, the internal procedures and guidance are covered by the configuration management.

O.Config-Control: The site applies a release procedure for the setup of the production and/or development process for each new product. In addition, the site has a process to classify and introduce changes for services and/or processes of released products. Minor changes are handled by the site, major changes must be acknowledged by the client. A designated team is responsible for the release of new products and for the classification and release of changes. This team comprises specialists for all aspects of the services and/or processes. The services and/or processes can be changed by authorised personnel only. Automated systems support configuration management and production control.

O.Config-Process: The site controls its services and/or processes using a configuration management plan. The configuration management is controlled by tools and procedures for the development and production of the product, for the management of flaws and optimisations of the process flow as well as for the documentation that describes the services and/or processes provided by a site.

O.Acceptance-Test: The site delivers configuration items that fulfil the specified properties. Parameter checks, functional and/or visual checks and tests are performed to ensure the compliance with the specification. The test results are logged to support tracing and the identification of systematic failures.

O.Organise-Process: For the configuration, pre-personalisation, initialisation or personalisation process it is ensured that the specified process is applied. The data integrity is controlled. Keys and other sensitive data can only be constructed by at least two employees. The operation is applied in crypto-boxes or similar devices. After the release process changes are only applied based on the request of the client. The update is done according to a controlled process.

O.Staff-Engagement: All employees who have access to sensitive configuration items and who can move parts of the product out of the defined production/development flow are checked regarding security concerns and have to sign a nondisclosure agreement. Furthermore, all employees are trained and qualified for their job.

O.Zero-Balance: The site ensures that all sensitive products ("intended TOE" of different clients) are separated and traced on a device basis. Automated control and/or two employees acknowledgement during hand over is applied for functional and defective devices. According to the agreed production flow the defect devices are either destroyed at the site or sent to the client or the consumer.

O.Reception-Control: Upon reception of any product/mask/"intended TOE" an immediate incoming inspection is performed. The inspection comprises the received amount, their identification and the assignment of the items to a related internal process.

O.Internal-Shipment: The recipient of a physical configuration item is identified by the assigned client address. The internal shipment procedure is applied to the configuration item. The address for shipment can only be changed by a controlled process. The packaging is part of the defined process and applied as agreed with the

client. The forwarder supports the tracing of configuration items during internal shipment. For every sensitive configuration item, the protection measures against manipulation are defined.

O.External-Delivery: The recipient of a physical configuration item is identified by the assigned consumer address. The external delivery procedure is applied to the sensitive configuration item. A delivery address is assigned to each product and subject of a controlled process. The packaging is also part of the defined process and applied as specified by the client. The forwarder supports the tracing of sensitive configuration items during external delivery. For every configuration item, the protection measures against manipulation are defined.

O.Data-Transfer: Sensitive electronic configuration items (data or documents in electronic form) are protected with cryptographic algorithms to ensure confidentiality and integrity. The associated keys must be assigned to individuals to ensure that only authorised employees are able to extract the sensitive electronic configuration item. The keys are exchanged based on secure measures and they are sufficiently protected.

O.Control-Scrap: The site has either measures in place to destruct sensitive documentation, erase electronic media and destroy sensitive configuration items so that they do not support an attacker, or the site returns the assets to be scrapped to the client, according to the secure shipment procedure of the client.

5.1 Security Objectives Rationale

The SST includes a Security Objectives Rationale with two parts. The first part includes the tracing which shows how the threats and OSPs are covered by the Security Objectives. The second part includes a justification that shows that all threats and OSPs are effectively addressed by the Security Objectives.

Note that the assumptions of the SST cannot be used to cover any threat or OSP of the site. They are pre-conditions fulfilled either by the site providing the sensitive configuration items or by the site receiving the sensitive configuration items. Therefore, they do not contribute to the security of the site under evaluation.

5.1.1 Mapping of Security Objectives

All the given security objective(s) in the table below counter(s) the threat / OSP.

Table 1. Security Problem Definition mapping to Security Objective

Security Problem Definition / Threats	Security Objective
T.Smart-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security
T.Rugged-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security
T.Computer-Net	O.Exclusive-Access O.Maintain-Security O.Network-Separation O.Logical-Access
T.Accident-Change	O.Logical-Access O.Logical-Operation O.Config-Items O.Config-Control O.Config-Process

Table 1. Security Problem Definition mapping to Security Objective...continued

Security Problem Definition / Threats	Security Objective
	O.Acceptance-Test O.Staff-Engagement O.Zero-Balance O.Control-Scrap
T.Unauthorised-Staff	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Logical-Operation O.Staff-Engagement O.Zero-Balance O.Control-Scrap
T.Staff-Collusion	O.Internal-Monitor O.Maintain-Security O.Staff-Engagement O.Zero-Balance O.Control-Scrap
T.Attack-Transport	O.LifeCycle-Doc O.Internal-Shipment O.External-Delivery
Security Problem Definition / Policies	Security Objective
P.Config-IT_Env	O.Config-IT_Env
P.LifeCycle-Doc	O.LifeCycle-Doc
P.Config-Items	O.Config-Items O.Reception-Control
P.Config-Control	O.Logical-Access O.Config-Items O.Config-Control
P.Config-Process	O.Config-Process
P.Reception-Control	O.Reception-Control
P.Accept-Product	O.Config-Control O.Config-Process O.Acceptance-Test
P.Zero-Balance	O.Staff-Engagement O.Zero-Balance O.Control-Scrap
P.Organise-Product	O.Logical-Access O.Logical-Operation O.Config-Control O.Config-Process O.Organise-Process
P.Product-Transport	O.Config-Process O.Internal-Shipment

Table 1. Security Problem Definition mapping to Security Objective...continued

Security Problem Definition / Threats	Security Objective
	O.External-Delivery O.Data-Transfer
P.Data-Transfer	O.Data-Transfer
P.Scrap-Items	O.Control-Scrap

5.1.2 Objectives Rationale

The following rationale provides a justification that shows that all threats and OSP are effectively addressed by the Security Objectives.

O.Config-IT_Env: The site uses only project related tools and IT equipment. To provide a separation between different projects, the site uses configuration file versioning and unique repositories as well as configuration management systems.

This directly addresses the OSP P.Config-IT_Env.

O.Exclusive-Access: Using the protected security networks is only possible from inside the certified security areas or via VPN tunnel in specific cases. Administrative tasks can only be executed by authorized personnel from specific security rooms. No other possibility does exist to access or administrate the security networks.

This directly addresses the threat T.Computer-Net.

O.LifeCycle-Doc: Dedicated documents exist which define the use and the management of the configuration management systems, the configuration item list, the site security , the production/development process and the production/development tools. The site follows the procedures and instructions of these documents.

This directly addresses the OSP P.LifeCycle-Doc. The threat T.Attack-Transport can be prevented.

O.Physical-Access: The site implements a "need to know" principle by separation measures using a combination of physical partitioning together with technical and organisational security measures. The access control measures support the enforcement of the separation and the "need to know" principle. The handling of assets is restricted to separate security areas.

By the combination of these measures the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff can be prevented.

O.Security-Control: The site is using dedicated, trained security personnel for guard services. These personnel are responsible for operation of the access control and alarm systems, performing patrol rounds, visitor registration, physical key management, the surveillance of the technical alarm sensors and the responses to incidents.

By the combination of these measures the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff can be prevented.

O.Alarm-Response: In case of an access attempt to an asset by an unauthorized person, the site has an alarm system in place. After the alarm is triggered the unauthorised person still must overcome further security measures. The reaction time of the employees and/or guards is short enough to prevent a successful attack.

By the combination of these measures the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff can be prevented.

O.Internal-Monitor: Regular meetings are implemented to monitor security incidences as well as changes or updates of security relevant systems and processes. This includes the assessment of security alarms and associated logs of the physical and logical protection. In addition, results of internal audits and assessments are reviewed.

This helps to prevent the threat(s) T.Smart-Theft, T.Rugged-Theft, T.Unauthorised-Staff and T.Staff-Collusion.

O.Maintain-Security: The security related surveillance and alarm systems are maintained on a regular basis. The physical and logical access permission are reviewed and updated if needed. Logs of the associated systems are reviewed to support the work.

This helps to prevent the threat(s) T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff and T.Staff-Collusion.

O.Network-Separation: The security network is located in a dedicated secured area. This network is connected only to dedicated trustworthy systems.

This directly addresses the threat T.Computer-Net.

O.Logical-Access: The secure IT network is split in several segments according to different security level and purpose (development, administration, lab, manufacturing). The protection of network segments is implemented according to the classification of the processed data. The separation is enforced by firewalls and additional network components. Network services are limited to prevent the misuse and the access to network segments. User accounts are limited to the access rights required by the job task following a strict "need to know principle".

This helps to address the OSP(s) P.Config-Control and P.Organise-Product. This helps to prevent the threat(s) T.Computer-Net and T.Accident-Change.

O.Logical-Operation: Virus protection and patch management for operating systems and applications ensure the secure operation of the computer systems and the defense against malfunctions provoked by malicious software. Furthermore, backup of the production control system and data processing tools is implemented and the classified data from the client is excluded from the backup.

This directly addresses the OSP P.Organise-Product. This helps to prevent the threat(s) T.Unauthorised-Staff and T.Accident-Change.

O.Config-Items: The different items part of an "intended TOE" and the "intended TOE" itself is under configuration management. This configuration management system assigns unique identification numbers.

This helps to address the OSP(s) P.Config-Items and P.Config-Control. This helps to prevent the threat T.Accident-Change.

O.Config-Control: "Intended TOE" development is performed by authorized people using configuration management plan and change management. Automated tools are used for configuration management and for production control.

This helps to address the OSP(s) P.Accept-Product, P.Organise-Product and P.Config-Control. This helps to prevent the threat T.Accident-Change.

O.Config-Process: The control of the released production/development processes and the controlled introduction of changes ensure a reproducible and consistent production/development. Procedures for setting up the production/development process as well as changes to the released processes and documents are in place. Changes can only be done by authorised personnel. A team of specialists ensures that all aspects are covered for the introduction of new processes and for the assessment of changes. All documentation is under configuration management.

This helps to address the OSP(s) P.Product-Transport, P.Accept-Product, P.Organise-Product and P.Config-Process. This helps to prevent the threat T.Accident-Change.

O.Acceptance-Test: The data processing and manufacturing process includes verification steps. Several times the resulting data from the data processing is verified by the client and the manufactured results are verified against the design data and the requirement specification of the client.

This directly addresses the OSP P.Accept-Product. This helps to prevent the threat T.Accident-Change.

O.Organise-Process: For the development/production process it is ensured that the specified process is applied. The data integrity is controlled. Keys and other sensitive data can only be constructed by at least two employees. The operation is applied in crypto-boxes or similar devices. The operation of cryptographic keys and

other sensitive data is applied in protected environments only. Sensitive data only needed for de-bugging and testing purposes is generated in a secure environment and is not used in (or for) the "intended TOE". After the release, process changes are only applied based on the request of the client. The update is done according to a controlled process.

This directly addresses the OSP P.Organise-Product.

O.Staff-Engagement: The site has established personnel security measures. All employees who have access to assets are checked regarding security concerns and have to sign a non-disclosure agreement. This provides legal liability to protect the assets against disclosure. Furthermore, all employees are qualified for their job, are trained and had to pass a questionnaire to check the security awareness.

This directly addresses the OSP P.Zero-Balance. This helps to prevent the threat(s) T.Accident-Change, T.Unauthorised-Staff and T.Staff-Collusion.

O.Zero-Balance: The security of scrap handling is ensured by either securely destruct assets (e.g. paper shredder) or return them to the client. Furthermore, in case of production, all assets are uniquely identified throughout the whole process. Before an order is closed a zero-balance calculation is documenting the good and bad parts of this order.

This directly addresses the OSP P.Zero-Balance. This helps to prevent the threat(s) T.Accident-Change, T.Unauthorised-Staff and T.Staff-Collusion.

O.Reception-Control: When design/test/production data is received, the integrity and completeness of the data is verified and assigned to the related client order. The link between data and client order ensures the unique identification. When receiving physical assets, an inspection of the items is performed in order to acknowledge the correct amount, their identification and the assignment. Received assets are registered within the tracking system.

This helps to address the OSP(s) P.Reception-Control and P.Config-Items.

O.Internal-Shipment: Packing procedures including seal tape and the tracking of the transport support the identification of manipulations during the transport. The address of the client is part of the product setup and included in the requirements specification of the client.

This directly addresses the OSP P.Product-Transport. The threat T.Attack-Transport can be prevented.

O.External-Delivery: Packing procedures including seal tape and the tracking of the transport support the identification of manipulations during the transport. The address of the customer/consumer is part of the product setup.

This directly addresses the OSP P.Product-Transport. The threat T.Attack-Transport can be prevented.

O.Data-Transfer: The integrity and confidentiality of the data transfer from/to the site is protected against modification and/or disclosure by cryptographic means during transfer. The selected cryptographic algorithms are appropriate to resist against high attack potential. Cryptographic keys and password used for secure communication are sufficiently protected against unauthorised access and disclosure.

This helps to address the OSP P.Product-Transport P.Data-Transfer.

O.Control-Scrap: The security of scrap handling is ensured by either securely destruct assets at the site (e.g. paper shredder) or return them to the client. Scrap material is stored, until destruction or shipment back to the client, in security environments. Procedures document the destruction process.

This helps to address the OSP(s) P.Zero-Balance and P.Scrap-Items. This helps to prevent the threat(s) T.Accident-Change, T.Unauthorised-Staff and T.Staff-Collusion.

6 Extended Assurance Components Definition

No extended components are defined in this Site Security Target.

7 Security Assurance Requirements

Clients using this Site Security Target require a TOE evaluation up to evaluation assurance level EAL6, potentially claiming conformance with the Eurosmart Protection Profile [\[3\]](#).

The Security Assurance Requirements (SAR) are:

- CM capabilities (ALC_CMC.5)
- CM scope (ALC_CMS.5)
- Delivery (ALC_DEL.1)
- Development Security (ALC_DVS.2)
- Life-cycle definition (ALC_LCD.1)

The Security Assurance Requirements listed above fulfil the requirements of [\[10\]](#) because hierarchically higher components than the defined minimum site requirements (ALC_CMC.3, ALC_CMS.3, ALC_DVS.1) are used in this Site Security Target.

In addition, the minimum set of SARs is extended by SAR of the assurance components for "CM capabilities" (ALC_CMC.5), "CM scope" (ALC_CMS.5), "Delivery" (ALC_DEL), "Development Security" (ALC_DVS.2), "Life-cycle definition" (ALC_LCD.1), .

7.1 Application Notes and Refinements

The description of the site certification process [\[10\]](#) includes specific application notes. The main item is that a product that is considered as "intended TOE" is not available during the evaluation. Since the term "TOE" is not applicable in the Site Security Target, the associated processes for the handling of products, or "intended TOEs" are in the scope of this Site Security Target and are described in this document. These processes are subject of the evaluation of the site.

The SST in hand has been refined to consider "intended TOEs" rather than specific TOEs. All other refinements as stipulated by the corresponding subsections in "Application Notes for Site Certification" [\[10\]](#), chapter 5 of the chosen [Assurance Classes](#) have been applied as well. In addition, the relevant refinements of the Eurosmart PP [\[3\]](#) have been considered.

7.2 Security Assurance Rationale

The Security Assurance Rationale maps the content elements of the selected assurance components of [\[5\]](#) to the Security Objectives defined in this SST. The refinements described above are considered.

The site has a process in place to ensure an appropriate and consistent identification of the products. If the site already receives configuration items, this process is based on the assumption that the received configuration items are appropriately labelled and identified.

Note: The content elements that are changed from the original CEM [\[8\]](#) according to the application notes in the process description [\[10\]](#) are written in italic. The term TOE can be replaced by "configuration items" in most cases. In specific cases it is replaced by "intended TOE". "Configuration items" is used here in the sense that these are items contributing to build or to produce the TOE.

The SAR Rationale does not explicitly address the developer action elements defined in [\[5\]](#) because they are implicitly included in the content elements. This comprises the provision of the documentation to support the evaluation and the preparation for the site visit. This includes the requirement that the procedures are applied as written and explained in the documentation.

7.2.1 Rationales, Aspects and References for ALC_CMC.5

ALC_CMC.5.1C - *The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling.*

Security Objective	Rational
O.Reception-Control	Ensures the correct identification of the incoming items.
O.Config-IT_Env	A CM-Plan which is mandatory for each project ensures appropriate and consistent labeling through its application.
O.LifeCycle-Doc	The provided tools include a configuration management system for versioning and bug tracking.

Aspects	Reference
The sources are labelled in the version control system, which is owned by CCC&S. Documents are labelled with a DOC-number, -title, -owner and date. Configuration Items are identified via the identifiers that are automatically provided by the system as well as the baseline labels that are given by the configuration manager.	<ul style="list-style-type: none"> - NXPOMS-999116894-3989 - L-BL CS BCaM Handbook, slide on Configuration management - Configuration Management References and Templates

ALC_CMC.5.2C - *The CM documentation shall describe the method used to uniquely identify the configuration items.*

Security Objective	Rational
O.LifeCycle-Doc	The method used to uniquely identify the configuration items is described in the CM-Plan.

Aspects	Reference
All items can be uniquely identified by the version control system, which is owned by CCC&S. Documents can be uniquely identified using the labelling described above. Configuration Items are identified via the identifiers that are automatically provided by the system as well as the baseline labels that are given by the configuration manager.	<ul style="list-style-type: none"> - NXPOMS-999116894-3989 - L-BL CS BCaM Handbook, slide on Configuration management - Configuration Management References and Templates

ALC_CMC.5.3C - *The CM documentation shall justify that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.*

Security Objective	Rational
O.LifeCycle-Doc	The adequate and appropriate acceptance procedures for configuration items are described in the CM-Plan.

Security Objective	Rational
O.Config-Control	Change acceptance is managed by authorized people only.

Aspects	Reference
Review board is in place for every project. Steering is done by CCC&S.	<ul style="list-style-type: none"> - NXPOMS-999116894-3989 - L-BL CS BCaM Handbook, slide on Configuration management, Change Control Board - CCB & Change Control Process Outline - NXPOMS-999116894-3989 - L-BL CS BCaM Handbook, slide on Configuration management, slide on NPI 3.0 Key Review overview - NPI Lifecycle - Configuration Management References and Templates - NXPOMS-1719007347-2486 - L-BL CS Gate Checklist

ALC_CMC.5.4C - The CM system shall uniquely identify all configuration items.

Security Objective	Rational
O.Config-IT_Env	Provides the CM system.
O.Config-Items	The configuration management system is ensuring uniqueness of the identification.
O.Config-Process	Unique identification of all configuration items is realized by performing the configuration management activities.
O.LifeCycle-Doc	All actions are performed in accordance with the CM-Plan.

Aspects	Reference
All items can be uniquely identified by the version control system, which is owned by CCC&S.	<ul style="list-style-type: none"> - NXPOMS-999116894-3989 - L-BL CS BCaM Handbook, slide on Configuration management - Configuration Management References and Templates

ALC_CMC.5.5C - The CM system shall provide automated measures such that only authorised changes are made to the configuration items.

Security Objective	Rational
O.Config-IT_Env	Provides the CM system.
O.Config-Items	The CM system ensure unique identification.
O.Config-Process	Mandates a CM-Plan for each project, and ensures that only authorized changes are made to the configuration items.

Security Objective	Rational
O.Config-Control	Ensures that only authorized changes are made to the configuration items.
O.Organise-Process	Ensures that only authorized changes are made to the configuration items according to the processes.
O.LifeCycle-Doc	Enforces the configuration management process.

Aspects	Reference
Different CM tools like DesignSync, CollabNet as well as EnoviaNXP provide automated measures to only allow authorized changes to configuration items. Restricted access allows only authorized persons to do changes and the authorization for the change is approved by the Change Control Board using the change process.	- NXPOMS-999116894-3989 - L-BL CS BCaM Handbook, slide on Configuration management
	- Configuration Management References and Templates
	- NXPOMS-999116894-4839 - Project Setup in Collabnet Instructions

ALC_CMC.5.6C - The CM system shall support the production of the *intended* TOE by automated means.

Security Objective	Rational
O.Acceptance-Test	Provides automated testing of the functionality.
O.Config-IT_Env	Provides the CM system.
O.Config-Items	The CM system ensure unique identification.
O.Config-Process	Mandates a CM-Plan for each project.
O.LifeCycle-Doc	Enforces the configuration management process and the automated means.
O.Zero-Balance	Zero-Balancing is performed at each step.

Aspects	Reference
Different CM tools like DesignSync, CollabNet as well as EnoviaNXP support the development of the "intended TOE" by automated means.	- NXPOMS-999116894-3989 - L-BL CS BCaM Handbook, slide on Configuration management
	- Configuration Management References and Templates
	- NXPOMS-999116894-4839 - Project Setup in Collabnet Instructions
	- NXPOMS-1719007347-2657 - L-BL CS Design Environment Maintenance

ALC_CMC.5.7C - The CM system shall ensure that the person responsible for accepting a configuration item into CM is not the person who developed it.

Security Objective	Rational
O.LifeCycle-Doc	Ensures, that activities performed are such that the person responsible for accepting a configuration item into CM is not the person who developed it.
O.Config-Process	Mandates a CM-Plan for each project.

Aspects	Reference
Specific roles in tools are defined in a way that the person responsible for accepting a configuration item into CM is not the person who developed it. E.g. the role 'Documentation Office' publishes a document written by an 'Author' or the 'Integrator' generates the release of the "intended TOE", while the 'Developer' is responsible for the development of the "intended TOE" but cannot release it.	- NXPOMS-999116894-4839 - Project Setup in CollabNet instructions - Configuration Management Procedure - NXPOMS-999116894-14314 - L-BL CS Project Role Descriptions

ALC_CMC.5.8C - The CM system shall identify the configuration items that comprise the TSF.

Security Objective	Rational
O.Config-IT_Env	Provides the CM system.
O.Config-Items	The CM system ensure unique identification.
O.Config-Process	Mandates a CM-Plan for each project.
O.LifeCycle-Doc	The CM-Plan identifies the configuration items that comprise the TSF supported by the configuration management system.

Aspects	Reference
Per [10] there is no specific TOE in the focus, therefore, this is only applicable to the CM documentation. The documentation can be identified in the tool EnoviaNXP.	- Product/project specific CM plans and the CI list that is used for CC evaluation

ALC_CMC.5.9C - The CM system shall support the audit of all changes to the *intended* TOE by automated means, including the originator, date, and time in the audit trail.

Security Objective	Rational
O.Acceptance-Test	Provides automated testing of the functionality.
O.Config-IT_Env	Provides the CM system.
O.Config-Items	The CM system ensure unique identification.

Security Objective	Rational
O.Config-Process	Mandates a CM-Plan for each project.
O.LifeCycle-Doc	As described in the CM-Plan the configuration management systems are configured such that an audit trail (showing originator, date and time) is automatically generated.

Aspects	Reference
Different CM tools like DesignSync or CollabNet provide automated means to support the audit of all changes. Documents stored in EnoviaNXP or NXPOMS are under version control.	<ul style="list-style-type: none"> - NXPOMS-1719007347-2015 - Enovia Basic Type Lifecycle Management - NXPOMS-1719007347-2524 - BL CS Configuration and Data Management Procedure - NXPOMS-999116894-4839 - Project Setup in Collabnet Instructions - NXPOMS-1719007347-4053 - OMS Admin Work Instruction for Site Security and other Confidential Documents

ALC_CMC.5.10C - The CM system shall provide an automated means to identify all other configuration items that are affected by the change of a given configuration item.

Security Objective	Rational
O.Config-IT_Env	Provides the CM system.
O.Config-Items	The CM system ensure unique identification.
O.Config-Process	Mandates a CM-Plan for each project.
O.LifeCycle-Doc	As described in the CM-Plan the CM system and software installed on the development workstations and servers provide automated means to identify all other configuration items that are affected by the change of a given configuration item.

Aspects	Reference
In case a source file has been changed, the code is compiled again, and all affected items are identified as they are marked as 'changed' compared with the version in the CM system.	<ul style="list-style-type: none"> - NXPOMS-1719007347-2524 - BL CS Configuration and Data Management Procedure - NXPOMS-999116894-4839 - Project Setup in Collabnet Instructions - Configuration Management Procedure - Requirements Engineering Procedure

ALC_CMC.5.11C - The CM system shall be able to identify the version of the implementation representation from which the *intended* TOE is generated.

Security Objective	Rational
O.Config-IT_Env	Provides the CM system.
O.Config-Items	The CM system ensure unique identification.
O.Config-Process	Mandates a CM-Plan for each project.
O.LifeCycle-Doc	The version of the implementation representation from which the "intended TOE" is generated can be determined through baselines.

Aspects	Reference
Different CM tools like DesignSync or CollabNet provide means to tag (baseline) a released version from which the "intended TOE" is generated. The version information of documents is stored in EnoviaNXP or NXPOMS.	<ul style="list-style-type: none"> - NXPOMS-1719007347-2015 - Enovia Basic Type Lifecycle Management - NXPOMS-1719007347-2524 - BL CS Configuration and Data Management Procedure - NXPOMS-999116894-4839 - Project Setup in Collabnet Instructions - NXPOMS-999116894-3989 - L-BL CS BCaM Handbook, slides referring to Baselines - Configuration Management Procedure - Requirements Engineering Procedure

ALC_CMC.5.12C - The CM documentation shall include a CM plan.

Security Objective	Rational
O.Config-Process	Mandates a CM-Plan for each project.

Aspects	Reference
Each project must have a project specific CM plan.	<ul style="list-style-type: none"> - NXPOMS-999116894-3989 - L-BL CS BCaM Handbook, slide on Configuration management - Product specific configuration management plan (CMP) available

ALC_CMC.5.13C - The CM plan shall describe how the CM system is used for the development of the *intended* TOE.

Security Objective	Rational
O.LifeCycle-Doc	The life-cycle documentation describes how the CM system is used for the development of the product.

Aspects

Reference

The development environment used is set up centrally as documented. Each project must create a project specific CM plan.

- NXPOMS-999116894-4839 - Project Setup in CollabNet instructions
- NXPOMS-999116894-3989 - L-BL CS BCaM Handbook, slide on Configuration management
- Product specific configuration management plan (CMP) available

ALC_CMC.5.14C - The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the *intended* TOE.

Security Objective

Rational

O.LifeCycle-Doc

The acceptance procedures for modified or newly created configuration items are described in the CM-Plan.

O.Config-Control

Mandates a CM-Plan for each project.

Aspects

Reference

The development environment used is set up centrally to ensure 'separation of duties'. Each project must have a project specific CM plan where the project specific CCB is described. Documents are managed centrally after initial creation by the 'Documentation Officer'.

- NXPOMS-999116894-4839 - Project Setup in CollabNet instructions
- NXPOMS-999116894-3989 - L-BL CS BCaM Handbook, slide on Configuration management and Change Control Board - CCB
- Product specific configuration management plan (CMP) available

ALC_CMC.5.15C - The evidence shall demonstrate that all configuration items are being maintained under the CM system.

Security Objective

Rational

O.LifeCycle-Doc

All configuration items are under configuration system and listed in the CI-list.

O.Config-Process

Ensures, that all configuration items are under version control.

Aspects

Reference

The development environment used is set up centrally to ensure 'separation of duties'. Each project must have a project specific CM plan where the project specific processes are described. Documents are stored in project vaults. Evidences can be provided during a site visit.

- NXPOMS-999116894-4839 - Project Setup in CollabNet instructions
- NXPOMS-999116894-3989 - L-BL CS BCaM Handbook, slide on Configuration management
- Product specific configuration management plan (CMP) available and documentation

ALC_CMC.5.16C - The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

Security Objective	Rational
O.Config-IT_Env	Provides the CM system.
O.Config-Process	Ensures, that all configuration items are under version control.
O.LifeCycle-Doc	The CI-list is generated from the CM systems.

Aspects	Reference
After the development environment used is set up centrally, each project must have a project specific CM plan where the project specific processes are described. Documents are stored in project vaults. Evidences can be provided during a site visit.	- NXPOMS-999116894-3989 - L-BL CS BCaM Handbook, slide on Configuration management - Product specific configuration management plan (CMP) available and documentation

The security assurance requirements of the assurance class "CM capabilities" listed above are suitable to support the production of complex products due to the formalized acceptance process and the automated support. The identification of all configuration items supports an automated and industrialized production process. The requirement for authorized changes supports the integrity and confidentiality required for the products. Therefore, this assurance level meets the requirements for the configuration management.

7.2.2 Rationales, Aspects and References for ALC_CMS.5

The scope of the evaluation according to the assurance class ALC_CMS comprises the security products, the complete documentation of the site provided for the evaluation and the configuration and initialization data as well as associated tools. The specifications and descriptions provided by the client are not part of the configuration management at the certified site.

ALC_CMS.5.1C - The configuration list includes the following: the *intended* TOE itself; the evaluation evidence required by the SARs in the ST; the parts that comprise the *intended* TOE; the implementation representation; security flaws; and development tools and related information. The CM documentation shall include a CM plan.

Security Objective	Rational
O.LifeCycle-Doc	The life-cycle documentation includes a CI-List which contains all the items of this content element.

Aspects	Reference
In terms of site certification, the configuration list is represented by the list of all applicable documents including this SST.	- SST - Document list/Bibliography

ALC_CMS.5.2C - The configuration list shall uniquely identify the configuration items.

Security Objective	Rational
O.LifeCycle-Doc	The CI-List uniquely identifies the configurations items per version, date, NXPOMS number, Collabnet ID (whatever is applicable per CI).

Aspects	Reference
All configuration items are maintained in the CM systems. Every document can be uniquely identified by version, date, NXPOMS number, Collabnet ID (whatever is applicable per CI).	- NXPOMS-1719007347-4053 - OMS Admin Work Instruction for Site Security and other Confidential Documents - CollabNet TeamForge - User & Administration Guide

ALC_CMS.5.3C - For each TSF relevant configuration item, the configuration list shall indicate the developer/*subcontractor* of the item.

Security Objective	Rational
O.LifeCycle-Doc	The CI-List indicates the developer/subcontractor/author for each configuration item.

Aspects	Reference
In terms of site certification, the CI-list is the list of all applicable documents. In the CI-List the author of each item is listed.	- Document list/Bibliography

The security assurance requirements of the assurance class "CM scope" listed above support the control of the production and test environment. This includes product related documentation and data as well as the documentation for the configuration management and the site security measures. Since the site certification process focuses on the processes based on the absence of a concrete TOE these assurance requirements are suitable.

7.2.3 Rationales, Aspects and References for ALC_DEL.1

ALC_DEL.1.1C - The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the *intended* TOE to the consumer.

Security Objective	Rational
O.Reception-Control	This ensures correct identification and labelling of received products or parts of a product.
O.External-Delivery	O.External-Delivery: This supports integrity and confidentiality by use of trustworthy transport, transport protection and recipient pre-notification and confirmation procedures.

Aspects	Reference
Ensuring integrity of physical items of an "intended TOE" sent to the consumer.	- NXPOMS-1719007347- 2652 - Site Security Manual - NXP Semiconductors ATBK - NXPOMS-1719007347-2354 – CCC&S Packing and Delivery Requirements for Security Products

The security assurance requirement of the assurance class "Delivery" listed above is suitable to define a controlled process for delivery products to the consumer. The confidentiality and integrity of the product during transport is addressed by this assurance class. Since the Protection Profile [3] requires the same assurance level it is enough.

7.2.4 Rationales, Aspects and References for ALC_DVS.2

ALC_DVS.2.1C - The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the *intended* TOE design and implementation in its development environment.

Security Objective	Rational
O.LifeCycle-Doc	This covers the overall development security documentation.
O.Exclusive-Access	This covers the technical restrictions.
O.Physical-Access	This covers the physical measures.
O.Security-Control	This covers the organizational measures of the guard team.
O.Alarm-Response	This covers the physical measures and their alarm follow up by the guard team.
O.Internal-Monitor	This covers organizational measures by reviews and management attention.
O.Maintain-Security	This covers organizational measures by maintenance.
O.Network-Separation	This covers logical measures, esp. the network separation.
O.Logical-Operation	This covers logical measures and the user interaction with the security systems.
O.Logical-Access	This covers logical measures in the area of firewall and virus protection as well at patch management.
O.Internal-Shipment	This covers procedural measures of internal transport of security material.
O.Control-Scrap	This covers procedural measures of secure destruction of security material.
O.Staff-Engagement	This covers personnel measures.
O.Zero-Balance	This covers the procedural measure to ensure all security material is under control.

Security Objective	Rational
O.Data-Transfer	This covers logical measures related to cryptographic encryption and signature algorithms during electronic transfer of data.

Aspects	Reference
<ul style="list-style-type: none"> - Access control to development areas inside the building, surveillance, alarm system and guard services to prevent access to the security area for unauthorized persons - Operation of the physical security system, emergency procedures, incident handling and reporting - Tracing and control of Visitors, external suppliers and cleaning personnel - Internal storage of products in a strong room, handling of physical objects, zero balancing, disposal of security products - Trustworthiness and training of staff - Organizational measures to enforce security and alarm tracing - Personal accountability for products - Policies and procedures for the internal handling of confidential information - Network security measures to ensure logical protection and authentication to computer systems using username and password - Maintenance of security measures - Protection of the internal shipment - Destruction of sensitive documents, data, products and other items 	- NXPOMS-1719007347- 2652 - Site Security Manual - NXP Semiconductors ATBK

ALC_DVS.2.2C - The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the *intended* TOE.

Security Objective	Rational
O.Acceptance-Test	Ensures the integrity by automated testing of the finished products.
O.LifeCycle-Doc	The development security documentation justifies, that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the "intended TOE".

Aspects

Reference

The justification is provided in this site security target because it shows that all threats are addressed by the measures. In addition, the measures are monitored to control the effectiveness. Besides this the lifecycle documentation also provides a justification from a different angle.

- NXPOMS-1719007347- 2652 - Site Security Manual - NXP Semiconductors ATBK
- This SST, see [chapter 7.2 Security Assurance Rationale](#)

The security assurance requirements of the assurance class "Development security" listed above are required since a high attack potential is assumed for potential attackers. The configuration items and information handled at the site during development, production, testing, assembly and pre-personalization or personalization of the "intended TOE" can be used by potential attackers for the development of attacks. Any keys loaded into the "intended TOE" also support the security during the internal shipment or the external delivery. Therefore, the handling and storage of electronic keys must also be protected. Further on the Protection Profile [3] requires this protection for sites involved in the lifecycle of Security ICs development and production.

7.2.5 Rationales, Aspects and References for ALC_LCD.1

ALC_LCD.1.1C - The life-cycle definition documentation shall describe the model used to develop and maintain the *intended* TOE.

Security Objective

Rational

O.LifeCycle-Doc

The live-cycle documentation describes the model used to develop the "intended TOE".

Aspects

Reference

The "intended TOE" is developed and maintained as per NXP development process.

- NXPOMS-999116894-3989 - L-BL CS BCaM Handbook
- NXPOMS-1719007347-2486 - L-BL CS Gate Checklist

ALC_LCD.1.2C - The life-cycle model shall provide for the necessary control over the development and maintenance of the *intended* TOE.

Security Objective

Rational

O.LifeCycle-Doc

The life-cycle model as described in the life-cycle documentation ensures the necessary control over the development and maintenance of the "intended TOE".

Aspects

Reference

The development control of CCC&S provides the necessary control and compliance of the development environment in use.

- NXPOMS-999116894-3989 - L-BL CS BCaM Handbook
- NXPOMS-1719007347-2486 - L-BL CS Gate Checklist
- NXPOMS-999116894-4839 - Project Setup in Collabnet Instructions

The security assurance requirements of the assurance class "Life-cycle definition" listed above are suitable to support the controlled development and production process. This includes the documentation of these processes and the procedures for the configuration management. One site provides only a limited support of the described lifecycle for the development and production of Security ICs. However, the assurance requirements are suitable to support the application of the site evaluation results for the evaluation of an "intended TOE".

8 Site Summary Specification

Please refer for the rationales, aspects and references to the subchapters in [Section 7.2](#) for the different ALC classes.

8.1 Preconditions Required by the Site

This section includes justifications for the assumptions defined in the SST. These assumptions are relevant for the splicing process since they must be examined during the product evaluation. Especially aspects like the classification of items and the appropriate provision of specifications for the site must be verified by checking appropriate evidence (e.g. the set of specifications provided to the site with a site certificate) during the product evaluation.

Please also refer to the site visit checklist [\[11\]](#).

The following table explains the preconditions of the client that are required to ensure the security measures of the site in order to protect its assets.

Table 2. Preconditions of Assumptions

Assumption	Precondition
A.Secure-IT-Provisioning	To enable that the site participates in the development of products the client provides services to setup and maintain the necessary development environment (e.g. workstations, tools, test samples) and configuration management systems (e.g. user accounts in project repositories). The client also provides a secure connection between the IT equipment of the site and a secure remote IT infrastructure of the client. These services are provided by the client in a secure way in order to properly protect the assets of the site. This includes the enforcement of a trustworthy access policy to the site equipment and data using the secure connection based on a "need-to-know" principle.
A.Client-Agreements [Production]	To enable the site to execute the production of products, the client needs to provide specifications, maybe production recipes, maybe tools, acceptance criteria and information how to handle scrap material.
A.Client-Agreements [Test]	To enable the site to test the client's products, the client needs to provide test specifications, test programs, scripts, process parameters and acceptance criteria. Maybe even information about the classification of the material is important.
A.Client-Agreements [Warehouse]	To allow the site to provide the warehouse and shipping service, it is necessary that the relevant work and shipping instructions and procedures are trained, shared and kept up to date. Furthermore, changes to the relevant procedures require a notification of the relevant people. Information about the handling of scrap material is required, as well as proper details and classification of the material to be shipped.
A.Client-Agreements [Satellite]	To enable the site to participate in the development of products, the client needs to provide services to setup and maintain the necessary development environment (e.g. workstations, development tools, test samples). Further, the client needs to setup and maintain the used configuration management systems and provide a project specific CM plan. This includes the setup and maintenance of user accounts in the project repositories and other required configuration management tools. The client needs to agree about the configuration management methods and the usage of the configuration management tools. The configuration management methods and tools by the client ensure the correct handling of the configuration items according to Common Criteria.

Table 2. Preconditions of Assumptions...continued

Assumption	Precondition
	For each project setup, the client needs to agree on the activities to be performed by the site, the specifications of the input for the site and the acceptance of the results from the site. Regarding a destruction of certain physical assets, the client need to specify whether the scrap need to be destroyed by the site or need to be sent back to the client. In the latter case the client is responsible for the secure destruction of the assets.
A.Client-Agreements [FA]	To enable the site to analyse the product, product specific documentation is needed. When a product fails according to the client, the failure analysis process can use product specific information (=specifications) as provided by the client to execute the analysis.
A.Data-Transfer [Test]	The development and/or production process delivers securely test programs, test data, pre-personalization data and/or physical material.
A.Item-Identification	Before sending items to this site, the previous site must label it uniquely. Those unique identifiers can come from EnoviaNXP, Collabnet or other tools.
A.External-Delivery	External delivery can only take place based on an order in SAP and to addresses defined in SAP. The delivery method is described in the shipment and delivery documentation. The site had to be informed about correct delivery information.
A.Mask-Support [Assembly]	To allow the site to perform the assembly, the client must provide appropriate masks to the site. The masks have to be usable by the sites assembly process and must include identification data. Furthermore, an agreement about how to handle defect and obsolete masks must be setup.
A.Internal-Shipment	Internal shipment can only take place based on an order in SAP and to addresses defined in SAP. The shipment method is described in the shipment and delivery documentation. The site had to be informed about correct shipment information.
A.Product-Integrity	To ensure integrity of the devices they shall be in a mode that the self-protection is fully operational. The client has to ensure the proper configuration of those devices.

8.2 Services of the Site

Table 3. Services of the Site

Service of the Site	Explanation of the Service
S.IT_Support	<p>The site provides 1st and/or 2nd & 3rd level IT support to the client. This consists of activities such as:</p> <ul style="list-style-type: none"> • Ticket creation or 1st level telephone hotline • Remote support 2nd and 3rd level • Installation of Client Operating Systems • Remote installation of software upgrades and patches • Resolving problems and responding to incidents • Implementing approved IT Changes • Implementing approved Service Request <p><i>Dependencies:</i> S.Secure_Area must be fulfilled to ensure physical security</p> <p><i>Assumptions:</i> A.Secure-IT-Provisioning must be fulfilled for secure networks A.Client-Agreements [IT] must be fulfilled</p>

Table 3. Services of the Site...continued

Service of the Site	Explanation of the Service
S.Internal_Shipment	<p>The site uses a shipment method such that assurance of integrity is assured throughout transport of physical security objects. Thus, the site does not comply with ALC_DEL.1, but internal shipment is covered under ALC_DVS.2.</p> <p><i>Dependencies:</i> S.Secure_Area must be fulfilled to ensure physical security</p> <p><i>Assumptions:</i> A.Item-Identification must be fulfilled A.Internal-Shipment must be fulfilled</p>
S.Testing	<p>The site ensures a reproducible test process within the limits defined for the released wafer test process. Therefore relevant parameters are controlled during the test process. This is subject of the configuration management.</p> <p><i>Dependencies:</i> S.Secure_Area must be fulfilled to ensure physical security</p> <p><i>Assumptions:</i> A.Client-Agreements [Production] must be fulfilled</p>
S.External_Delivery	<p>This site provides the service of secure receipt, packing, storage and delivery to customers of following goods: wafers with ICs, semi-finished products containing these ICs and finished products (i.e. Smart Cards), and any related goods. The processes to be followed are provided by the client.</p> <p><i>Dependencies:</i> S.Secure_Area must be fulfilled to ensure physical security</p> <p><i>Assumptions:</i> A.Client-Agreements [Warehouse] must be fulfilled A.Item-Identification must be fulfilled A.External-Delivery must be fulfilled A.Product-Integrity must be fulfilled</p>
S.Scrapping	<p>This site provides a scrapping service for other sites having a business relationship with NXP, to hand in defect or rejected security items (e.g. finished, semi-finished, wafers, hard discs containing unencrypted data) which are destructed according to the defined secure destruction process.</p> <p><i>Dependencies:</i> S.Secure_Area must be fulfilled to ensure physical security</p> <p><i>Assumptions:</i> A.Client-Agreements [Warehouse] must be fulfilled A.Item-Identification must be fulfilled A.External-Delivery must be fulfilled Note: A.Product-Integrity does <u>not</u> need to be fulfilled</p>
S.IC_Packaging	<p>The site provides the services which covers parts of the life-cycle phase 4 related to the packaging and testing of wafer with security ICs. In detail, the site assembles security ICs and/or does wafer level chip packing.</p> <p><i>Dependencies:</i> S.Secure_Area must be fulfilled to ensure physical security</p> <p><i>Assumptions:</i> A.Item-Identification must be fulfilled A.Client-Agreements [Production] must be fulfilled A.Product-Integrity must be fulfilled</p>
S.Reliability_Testing_And_Characterization	<p>This site provides the service of product robustness characterization and reliability stress testing as needed at the end of the development phase but prior to product release.</p>

Table 3. Services of the Site...continued

Service of the Site	Explanation of the Service
	<p><i>Dependencies:</i> S.Secure_Area must be fulfilled to ensure physical security</p> <p><i>Assumptions:</i> A.Client-Agreements [Test] must be fulfilled A.Client-Agreements [FA] must be fulfilled A.Item-Identification must be fulfilled</p>
S.Failure_Analysis	<p>This site provides a service to find root causes of defects. This comprises analysis and de-bugging of samples, low yield devices and field returns. The site uses design data to support the activity. It does support the complaint handling and flaw remediation service.</p> <p><i>Dependencies:</i> S.Secure_Area must be fulfilled to ensure physical security</p> <p><i>Assumptions:</i> A.Secure-IT-Provisioning must be fulfilled for secure networks A.Client-Agreements [Test] must be fulfilled A.Client-Agreements [FA] must be fulfilled A.Item-Identification must be fulfilled</p>
S.Secure_Area	<p>The site provides a secure physical environment (RED and/or YELLOW area) for classified IT infrastructure and equipment installed by the client at the site according to Common Criteria requirements.</p> <p><i>Dependencies:</i> none</p> <p><i>Assumptions:</i> none</p>
S.Wafer-Treatment	<p>Optical inspection and wafer treatment (dicing, grinding and polishing).</p> <p><i>Dependencies:</i> S.Secure_Area must be fulfilled to ensure physical security</p> <p><i>Assumptions:</i> A.Data-Transfer [Test] must be fulfilled A.Item-Identification must be fulfilled A.Client-Agreements [Production] must be fulfilled</p>
S.Sample_Packaging	<p>The site assembles open/untested/final tested security ICs and/or wafers into chip packages for engineering purposes (e.g. project samples, engineering samples, customer samples).</p> <p><i>Dependencies:</i> S.Secure_Area must be fulfilled to ensure physical security</p> <p><i>Assumptions:</i> A.Item-Identification must be fulfilled A.Client-Agreements [Production] must be fulfilled A.Product-Integrity must be fulfilled</p>

9 Bibliography

- [1] Eurosmart. Site Security Target Template, Version 2.0, 15. April 2021.
- [2] a.) NXP Semiconductors. "CCC&S Security Objects", NXPOMS-1719007347-2401, 29. January 2024.
b.) NXP Semiconductors. "CCC&S Security Objects Master", NXPOMS-1719007347-2402, 02. January 2025.
- [3] Eurosmart. Security IC Platform Protection Profile with Augmented Packages (BSI-CC-PP-0084-2014), Version 1.0, 2014.
- [4] Common Criteria. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 2022, Revision 1, November 2022.
- [5] Common Criteria. Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, Version 2022, Revision 1, November 2022.
- [6] Common Criteria. Common Criteria for Information Technology Security Evaluation, Part 4: Framework for the specification of evaluation methods and activities, Version 2022, Revision 1, November 2022.
- [7] Common Criteria. Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements, Version 2022, Revision 1, November 2022.
- [8] Common Criteria. Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 2022, Revision 1, November 2022.
- [9] Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.1, July 2024.
- [10] Common Criteria. Supporting Document Guidance, Site Certification, Version 1.0, Revision 1, CCDB-2007-11-001, October 2007.
- [11] NXP Semiconductors. "Security Checklist for Site Visit", NXPOMS-1719007347-16672, 24. October 2024.

10 Glossary

CA – Certificate Authority

CC – Common Criteria

CCC&S – Competence Center Crypto & Security

CI – Configuration Item

CKC – Customer Key Creation (system for key creation and post-shipment services)

CL – Configuration List

CM – Configuration Management

CSH – China Secure High Confidential

CSM – China Secure Main Confidential

CSR – Certificate Signing Requests

CSx – China Secure - Main or High Confidential

CTO – Chief Technology Organization

DDS – Data Delivery Service

DIT – Data Intake and Translation

DIT – Data Intake

DMZ – Demilitarized Zone

DNV – Dynamic Non-volatile

EAL – Evaluation Assurance Level

FAE – Field Application Engineer

FH – Fabkey Helpdesk (old name of DNV desk)

FS – Facility Secure

HS – High Secure

HSM – Hardware Security Module

IC – Integrated Circuit

IP – Intellectual Property

KDS – Key Delivery Services

KIS – Key Insertion Server

MBK – Master Backup Key

NPIT – New Product Introduction Team

OEF – Order Entry Form

OSP – Organizational Security Policy

PP – Protection Profile

PMP – Project Management Plan

PQE – Product Quality Engineer

PS – Production Secure

PS-HS – Production Secure-High Secure

PS-RS – Production Secure-Restricted Secure

RCS – ROM Code System

ROM – Read-Only Memory

RS – Restricted Secure

SAR – Security Assurance Requirement

SNV – Static Non-Volatile

SNR – Serial Number Server

SSM – Site Security Manual

SST – Site Security Target

ST – Security Target

TOE – Target of Evaluation

TP – Trust Provisioning

TSM – Trusted Service Manager

Legal information

Definitions

Draft — A draft status on a document indicates that the content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included in a draft version of a document and shall have no liability for the consequences of use of such information.

Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Limiting values — Stress above one or more limiting values (as defined in the Absolute Maximum Ratings System of IEC 60134) will cause permanent damage to the device. Limiting values are stress ratings only and (proper) operation of the device at these or any other conditions above those given in the Recommended operating conditions section (if present) or the Characteristics sections of this document is not warranted. Constant or repeated exposure to limiting values will permanently and irreversibly affect the quality and reliability of the device.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at <https://www.nxp.com/profile/terms>, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

No offer to sell or license — Nothing in this document may be interpreted or construed as an offer to sell products that is open for acceptance or the grant, conveyance or implication of any license under any copyrights, patents or other industrial or intellectual property rights.

Quick reference data — The Quick reference data is an extract of the product data given in the Limiting values and Characteristics sections of this document, and as such is not complete, exhaustive or legally binding.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Suitability for use in non-automotive qualified products — Unless this document expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications.

In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

Translations — A non-English (translated) version of a document, including the legal information in that document, is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Security — Customer understands that all NXP products may be subject to unidentified vulnerabilities or may support established security standards or specifications with known limitations. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately.

Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP.

NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

Trademarks

NXP — wordmark and logo are trademarks of NXP B.V.

Notice: All referenced brands, product names, service names, and trademarks are the property of their respective owners.

Tables

Tab. 1.	Security Problem Definition mapping to Security Objective	15	Tab. 2.	Preconditions of Assumptions	35
			Tab. 3.	Services of the Site	36

Contents

1	Document Information	2
1.1	Reference	2
1.2	Revision History	2
2	SST Introduction	3
2.1	Identification of the Site	3
2.2	Site Description	3
2.2.1	Physical Scope	3
2.2.2	Logical Scope	3
2.2.3	List of services in Scope	4
3	Conformance Claim	6
4	Security Problem Definition	7
4.1	Assets	7
4.2	Threats	7
4.3	Organisational Security Policies	8
4.4	Assumptions	9
5	Security Objectives	13
5.1	Security Objectives Rationale	15
5.1.1	Mapping of Security Objectives	15
5.1.2	Objectives Rationale	17
6	Extended Assurance Components	
	Definition	20
7	Security Assurance Requirements	21
7.1	Application Notes and Refinements	21
7.2	Security Assurance Rationale	21
7.2.1	Rationales, Aspects and References for ALC_CMC.5	22
7.2.2	Rationales, Aspects and References for ALC_CMS.5	29
7.2.3	Rationales, Aspects and References for ALC_DEL.1	30
7.2.4	Rationales, Aspects and References for ALC_DVS.2	31
7.2.5	Rationales, Aspects and References for ALC_LCD.1	33
8	Site Summary Specification	35
8.1	Preconditions Required by the Site	35
8.2	Services of the Site	36
9	Bibliography	39
10	Glossary	40
	Legal information	42

Please be aware that important notices concerning this document and the product(s) described herein, have been included in section 'Legal information'.